UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* iPhone with Verizon wireless number 415-686-2112, per Attachment A	)	Case No. 1:23-mc 194

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

iPhone with Verizon wireless number 415-686-2112, per Attachment A attached hereto

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
13 U.S.C. § 305	Knowingly submit false or misleading export information
18 U.S.C. § 1001	False Declaration
16 U.S.C. § 470aaa-5	Offense under Paleontological Resources Preservation Act

The application is based on these facts:

See Affidavit which is attached hereto and incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jason Bulkley, SA, Bureau of Land Management
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 4:00pm a.m./p.m. *(specify reliable electronic means)*.

Date: March 3, 2023

Judge's signature

City and state: Eugene, Oregon

MUSTAFA T. KASUBHAI, United States Magistrate Judge
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF Jason Bulkley

Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize Evidence Including Digital Evidence

I, Jason Bulkley, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Bureau of Land Management and have been since October 2020. My current assignment is within the Office of Law Enforcement and Security, Region 3, Utah. My training and experience includes crimes relating to the theft and destruction of natural resources including paleontological resources, theft and damage/destruction to federal lands, resources and government property, fraud, conspiracy, and electronic communications.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the seizure, search, and examination of Noelle Toomajian's cellular telephone, iPhone with Verizon wireless number 415-686-2112 (hereinafter "Device"), as described in Attachment A hereto, and the extraction of electronically stored information from the Device, as described in Attachment B hereto. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute the evidence, fruits, and instrumentalities of violations of 13 U.S.C. § 305 (knowingly submitted false or misleading export information), 18 U.S.C. § 1001 (false declaration), 16 U.S.C. § 470aaa-5 (collecting offenses and false labeling offenses under the Paleontological Resources Preservation Act) , and 18 U.S.C. § 554 (smuggling goods from the United States)

3. This affidavit is intended to show only that there is sufficient probable cause for

the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. 13 U.S.C. § 305 provides that it is illegal to knowingly submit false or misleading export information; 18 U.S.C. § 1001 provides that it is illegal to make a false declaration, 16 U.S.C. § 470aaa-5 (the Paleontological Resources Preservation Act) provides that it is illegal to traffic paleontological resources illegally collected from public lands, and to false label said resources; 18 U.S.C. § 554 provides that it is illegal to smuggling goods from the United States.

Statement of Probable Cause

A. Background Regarding Trafficking of Dinosaur Bones

5. In or around April 2014, the BLM received a tip from Informant 1 that Seller 1, Seller 2, and Vint WADE took part in an illegal dinosaur-bone trafficking operation. Their operation consisted of Seller 1 illegally collecting, excavating, and removing dinosaur bone from federal lands and then selling the raw materials to WADE. Subsequent subpoenas yielded significant cell phone communications between the three individuals as well as several personal checks paid by WADE to Seller 1 and Seller 2 in the cumulative amount of $4,900 for “Rocks.” Informant 1 also provided pictures of illegally collected dinosaur bone.

6. In or around September 2016, BLM Ranger Greg Meuth issued mandatory appearance violations to Seller 3, Seller 4, and Seller 5 (who subsequently became Informant 2) for the illegal collection of dinosaur bone on BLM lands within the Canyon Country District Office in Utah. During the investigation, Informant 2 admitted selling dinosaur bone to WADE for one dollar per pound. Informant 2 also told investigators that WADE sold and shipped the bone to China.

7. In or around September 2016, the BLM received a report about Seller 6 collecting and selling dinosaur bone. The reporting party said Seller 6 was illegally collecting dinosaur bone from federal lands which seller 6 allegedly cut, polished, and sold. The reporting party also said Seller 6 dug up and collected a large dinosaur bone on federal land near Cortez, Colorado with other associates and sold it to WADE for $6,000. The BLM obtained a picture of the bone along with other dinosaur bones illegally collected from BLM lands. The reporting party provided photos of the cut and polished bones.

8. In November 2017 the BLM paleontologist reported the theft of a known/documented dinosaur leg bone in an area known as Yellow Cat on BLM administered lands. The BLM conducted a subsequent investigation however, no suspects were identified, and the case was eventually closed.

9. In or around 2019, the Grand County Sherriff's Office in Utah arrested Informant 2 and Seller 4 for drug-related activities. The Sherriff's Office informed the BLM that Informant 2 and Seller 4 were in possession of dinosaur bones and digging tools seized during the investigation. BLM Rangers Curtis Racker and Ranger Cody Marsh and SA Mike Hauck investigated the incident and interviewed both individuals. Informant 2 and Seller 4 were

eventually issued violation notices for removing paleontological and archaeological resources from BLM lands in Southeastern Utah. During an interview with Informant 2, Informant 2 admitted to the illegal collection and selling of dinosaur bone to WADE for years.

10. In February 2021, a concerned citizen reported the location of a dinosaur leg bone on BLM administered lands. They were concerned at the amount of footprints and vehicle traffic near the bone's location suggesting that it may be stolen. They provided a photo of the bone. The BLM investigated the situation but was unable to locate the bone. In January 2022, the citizen reported back to the BLM the bone had been taken and provided additional photos.

11. From on or about October 6, 2021, to on or about January 27, 2022, I communicated with Informant 1, who had firsthand knowledge about individuals who collected and sold dinosaur bone illegally obtained from BLM lands. Informant 1 told me they were present when Seller 1 illegally collected dinosaur bone from BLM lands. Informant 1 said Seller 1 would call WADE on his cell phone when Seller 1 had around five 5-gallon buckets of dinosaur bone and arrange a transaction. Informant 1 said they were present at 3090 S. Desert Rd, Moab, UT 84532 when WADE bought dinosaur bone from Seller 1 and other various sellers.

12. Informant 2 asserts that, in or around 2021, Informant 2 illegally collected 80-100 pounds of dinosaur bone from BLM lands. Informant 2 reported they later sold the bone to WADE for $2,000 in cash. According to Informant 2, WADE placed the bone into plastic containers with other dinosaur bone he was stockpiling awaiting shipment to China. WADE filled 55-gallon barrels and larger white plastic containers with dinosaur bone and kept them at his residential property until Wade could arrange shipment to China.

B. The CONEX

13. From on or about February 16, 2022, to the present, I communicated with Informants 1 and 2 who shared firsthand knowledge about individuals who illegally collected and sold dinosaur bone from BLM lands. On multiple occasions between February 16, 2022, and the present, Informants 1 and 2 admitted to illegally collecting dinosaur bone from BLM lands and selling it to both Seller 1 and WADE. Both informants have seen WADE place dinosaur bone into storage containers at his property in Moab, Utah.

14. From in or around July 2022 to in or around November 2022, I worked with investigators to obtain shipping information concerning WADE. According to Customs and Border Protection employees, who I spoke with as part of this investigation, WADE's last shipment to China occurred in 2020.

15. On or about November 8, 2022, I watched WADE and Wade's spouse Donna Wade (D. WADE) moving approximately five large white plastic containers holding suspected dinosaur bone at their property in Moab. At approximately 10:58 a.m., I saw a tractor trailer truck hauling the CONEX arrive at the property. The white plastic containers were loaded into the CONEX and the truck left the property. I also saw at least eight blue 55-gallon barrels with suspected dinosaur bone that remained on the property.

16. On or about November 17, 2022, I obtained shipping documents for the CONEX. The documentation listed the shipper as Wade's Wood & Rock, a company owned and operated by WADE and D. WADE. The documentation listed the contents as "stone ware." The documentation listed the pickup location as 3090 Desert Road, Moab, Utah 84532, and the final delivery destination as China.

17. On or about November 17, 2022, Customs and Border Protection ("CBP") told me that the CONEX arrived at the Long Beach terminal in California. CBP confirmed to me that the CONEX originated from WADE's property in Moab and that the shipper was Wade's Wood and Rocks.

18. On or about December 6, 2022, CBP agents inspected the contents of the CONEX at the Long Beach terminal, and it was determined that the materials listed as "stone ware" were, in fact, fossilized dinosaur bone. Alan Titus (a BLM paleontologist) and I were present for the inspection. Titus identified five containers of dinosaur bone, estimated to weigh 17,000 to 18,000 pounds.

19. On or about December 7, 2022, CBP agents called phone number (435) 260-2032 which was listed on the shipping invoice and talked to D. WADE about the contents of CONEX. The shipping invoice also lists "Wade's Rocks" with an address of 3090 S. Desert Rd, Moab, UT 84532. CBP asked D. WADE what the CONEX contained, and she stated it was mostly agate and a few pieces of jasper. CBP asked D. WADE if there was anything else in the CONEX and she indicated there was not. CBP then emailed wadesrocks@yahoo.com a PDF fillable form to verify D. WADE's statements. The form was digitally filled out, signed by "Donna Wade", and returned via the same email address. The form had the same basic information as her statements. The form lists the principal exporter/company name as "Wade's Wood & Rocks" located at 3090 S. Desert Rd, Moab, UT 84532. The form also lists the email address as wadesrocks@yahoo.com and the phone number as (435) 260-2032.

20. On or about December 7, 2022, I submitted for and obtained a search warrant in the Central District of California for the CONEX. I seized the five containers of dinosaur bone

totaling 17,354 pounds and transported them back to Utah where I processed them as evidence.

21. On or about January 10, 2023, I submitted for and obtained a search warrant in the District of Utah for Wade's Wood & Rock located at 3090 S. Desert Rd, Moab, UT 84532. As part of this warrant, I seized the cellular phone with the number (435) 260-2032 primarily used by D. WADE. During the analysis of this phone, I discovered several conversations with people trying to purchase dinosaur bone. I also discovered a conversation with an individual named "Noelle", phone number (415) 686-2112. Accurint phone and person reports identified her as Noelle Toomajian, a resident of Oregon, with a current address of 253 Cambridge St., Ashland, OR 97520. According to the text messages, Toomajian coordinated the exportation of the illegal bone and other materials in the CONEX searched and seized in California. Toomajian texted D. WADE (435-260-2032) and said that Toomajian would communicate information and pictures to the Wades regarding the materials in the CONEX, which I know to be illegally sold dinosaur bones.

22. On or about February 15, 2023, BLM SA Greg Filer went to 253 Cambridge St, Ashland, OR, and saw a vehicle with OR license plate 695-FXX pull into the driveway. The registered owner of the vehicle was Toomajian. SA Filer then saw a female matching her description get out of the vehicle and go into the house. SA Filer ran Toomajian through OR LEDS and NCIC and confirmed her address was 253 Cambridge St, Ashland, OR. The Accurint phone report only lists one phone for Toomajian, therefore the phone on her person is likely to be the phone authorized to be searched under this warrant.

23. The Accurint phone report only lists one phone for Toomajian; therefore, the

phone on her person is likely to be the Device authorized to be seized and searched under this warrant. Based on my training and experience, I know that most people possess their cell phones with them throughout the day, especially when outside of their residence and in the community. If the Device is not in Toomajian's possession at the time of law enforcement contact, I may seek an additional warrant to locate and seize the Device.

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

25. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a Wireless Telephone. In my training and experience,

examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and experience, I know:

a. Data on the Device can provide evidence of a file that was once on the Device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how

and when the device was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the device user. Last, forensic evidence on a device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its

use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

28. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

29. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

30. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file

system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

31. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

32. If the Device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

33. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

34. Based on the foregoing, I have probable cause to believe, and I do believe, that the Device described in Attachment A contains evidence, fruits, and instrumentalities of violations of 13 U.S.C. § 305, 18 U.S.C. § 1001, 16 U.S.C. § 470aaa-5, 18 U.S.C. § 554, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search and seizure of the Device described in Attachment A for the items listed in Attachment B and the

seizure and examination of any such items found.

35. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Ruth Hackford-Peer. I was informed that it is AUSA Hackford-Peer's opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

Request for Sealing

36. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may endanger the life or physical safety of an individual, cause flight from prosecution, cause destruction of or tampering with evidence, cause intimidation of potential witnesses, or otherwise seriously jeopardize an investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

/s/ Jason Bulkley, per rule 4.1
Jason Bulkley, Special Agent, BLM

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 4:30pm a.m/p.m. on March 3, 2023.

HONORABLE MUSTAFA T. KASUBHAI
United States Magistrate Judge

ATTACHMENT A

Property to be Searched and Seized

The property to be searched and seized is Noelle Toomajian's cellular telephone, an Apple IPhone with Verizon wireless number 415-686-2112. The property is believed to be in Noelle Toomajian's possession within the District of Oregon.

ATTACHMENT B

Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of 13 U.S.C. § 305, 18 U.S.C. § 1001, 16 U.S.C. § 470aaa-5, 18 U.S.C. § 554 and involve Noelle Toomajian since October 2021, including:

   a. Communication records and information describing or identifying the locations of paleontological resources and land ownership.

   b. Communication records and information showing sales, orders, and other aspects of trafficking paleontological resources.

   c. GPS tracks, data, and information regarding location information associated with the trafficking of paleontological resources.

   d. Documents, records, pictures, video, audio files, and information showing the sale or offer for sale of paleontological resources.

   e. Documents, records, pictures, video, audio files, and information regarding the shipping, exportation, and mislabeling of paleontological resources.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet, including:

   a. Records of Internet Protocol addresses used.

   b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user

entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data

falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. If the Device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.